Chief Information Officer

Office of Information Technology
Centers for Medicare & Medicaid Services

CMS Vulnerability Disclosure Policy

Issued:	April 24, 2019

Record of Changes

The table below capture changes when updating the document. All columns are mandatory.

Version Number	Date	Chapter Section	Author/Owner Name	Description of Change
1.0	*04/24/2019*	*All*	*ISPG*	*Initial Publication*

Effective Date/Approval

This policy becomes effective on the date that CMS' Chief Information Officer (CIO) signs it and remains in effect until it is rescinded, modified or superseded by another policy.

This policy must not be implemented in any recognized bargaining unit until the union has been provided notice of the proposed changes and given an opportunity to fully exercise its representational rights.

Signature: /s/

Rajiv Uppal
Chief Information Officer
Office of Information Technology

Policy Owner's Review Certification

This document must be reviewed in accordance with the established review schedule located on the CMS website.

Signature: /s/

George Hoffmann
Acting Director, Chief Information Security Officer
Office of Information Technology

Table of Contents

1. Purpose

This policy is intended to give security researchers clear guidelines for conducting vulnerability discovery activities directed at Centers for Medicare & Medicaid Services (CMS) websites, applications, and information systems, and submitting discovered vulnerabilities to CMS.

2. Overview

Maintaining the security of our networks is a high priority at CMS. Our information technologies provide critical services to serve Medicare & Medicaid beneficiaries. Ultimately, our network security ensures that we can accomplish our missions for Medicare & Medicaid beneficiaries and the health care providers who serve them.

The security researcher community regularly makes valuable contributions to the security of organizations and the broader Internet, and CMS recognizes that fostering a close relationship with the community will help improve our own security. So if you have information about a vulnerability in a CMS website, application, or information system, we want to hear from you!

Information submitted to CMS under this policy will be used for defensive purposes – to mitigate or remediate vulnerabilities in our networks or applications, or the applications of our vendors. This is CMS' initial effort to create a positive feedback loop between researchers and CMS – please be patient as we refine and update the process.

Please review, understand, and agree to the following terms and conditions before conducting any testing of CMS systems and before submitting a report.

3. Scope

Any public-facing website owned, operated, or controlled by CMS, including web applications hosted on those sites and Application Programming Interfaces (APIs).

4. How to Submit a Report

Please provide a detailed summary of the vulnerability, including: type of issue; product, version, and configuration of software containing the bug; step-by-step instructions to reproduce the issue; proof-of-concept; impact of the issue; and suggested mitigation or remediation actions, as appropriate to:
cms_it_service_desk@cms.hhs.gov

5. Guidelines

CMS will deal in good faith with researchers who discover, test, and submit vulnerabilities or indicators of vulnerabilities in accordance with these guidelines:

Your activities are limited exclusively to:

1. Testing to detect a vulnerability or identify an indicator related to a vulnerability; or
2. Sharing with, or receiving from, CMS information about a vulnerability or an indicator related to a vulnerability.

- You do no harm and do not exploit any vulnerability beyond the minimal amount of testing required to prove that a vulnerability exists or to identify an indicator related to a vulnerability.
- You avoid intentionally accessing the content of any communications, data, or information transiting or stored on CMS information system(s) – except to the extent that the information is directly related to a vulnerability and the access is necessary to prove that the vulnerability exists.
- You do not exfiltrate any data under any circumstances.
- You do not intentionally compromise the privacy or safety of CMS personnel or any third parties.
- You do not intentionally compromise the intellectual property or other commercial or financial interests of any CMS personnel or entities, or any third parties.
- You do not publicly disclose any details of the vulnerability, indicator of vulnerability, or the content of information rendered available by a vulnerability, except upon receiving explicit written authorization from CMS.
- You do not conduct denial of service testing.
- You do not conduct social engineering, including spear phishing, of CMS personnel or contractors.
- You do not submit a high-volume of low-quality reports.
- If at any point you are uncertain whether to continue testing, please engage with our team.

6. What You Can Expect From Us

We take every disclosure seriously and very much appreciate the efforts of security researchers. We will investigate every disclosure and strive to ensure that appropriate steps are taken to mitigate risk and remediate reported vulnerabilities.

CMS has a unique information and communications technology footprint which routinely handles medical and medical billing information. Many CMS technologies are involved in vital health care decisions and could have impact on beneficiaries and providers. CMS must take extra care while investigating the impact of vulnerabilities and providing a fix, so we ask your patience during this period.

CMS remains committed to coordinating with the researcher as openly and quickly as possible. This includes:

- Within three business days, we will acknowledge receipt of your report. CMS's security team will investigate the report and may contact you for further information.
- To the best of our ability, we will confirm the existence of the vulnerability to the researcher and keep the researcher informed, as appropriate, as remediation of the vulnerability is underway.
- We want researchers to be recognized publicly for their contributions, if that is the researcher's desire. We will seek to allow researchers to be publicly recognized whenever possible. However, public disclosure of vulnerabilities will only be authorized at the express written consent of CMS.

Information submitted to CMS under this policy will be used for defensive purposes – to mitigate or remediate vulnerabilities in our networks or applications, or the applications of our vendors. CMS may share your vulnerability reports with US-CERT, as well as any affected vendors or open source projects.

7. Legal

You must comply with all applicable Federal, State, and local laws in connection with your security research activities or other participation in this vulnerability disclosure program.

CMS does not authorize, permit, or otherwise allow (expressly or impliedly) any person, including any individual, group of individuals, consortium, partnership, or any other business or legal entity to engage in any security research or vulnerability or threat disclosure activity that is inconsistent with this policy or the law. If you engage in any activities that are inconsistent with this policy or the law, you may be subject to criminal and/or civil liabilities.

To the extent that any security research or vulnerability disclosure activity involves the networks, systems, information, applications, products, or services of a non-CMS entity (e.g., other Federal departments or agencies; State, local, or tribal governments; private sector companies or persons; employees or personnel of any such entities; or any other such third party), that non-CMS third party may independently determine whether to pursue legal action or remedies related to such activities.

If you conduct your security research and vulnerability disclosure activities in accordance with the restrictions and guidelines set forth in this policy, (1) CMS will not initiate or recommend any law enforcement or civil lawsuits related to such activities, and (2) in the event of any law enforcement or civil action brought by anyone other than CMS, CMS will take steps to make known that your activities were conducted pursuant to and in compliance with this policy.

CMS may modify the terms of this policy or terminate the policy at any time.